Q1 Team Name

0 Points

INSYNC

Q2 Commands

5 Points

List the commands used in the game to reach the ciphertext.

go
go
go
go
go
give
read

Q3 Analysis

30 Points

Give a detailed description of the cryptanalysis used to figure out the password. (Use Latex wherever required. If your solution is not readable, you will lose marks. If necessary the file upload option in this question must be used TO SHARE IMAGES ONLY.)

When we started level-7 on first screen we got message like "You enter a narrow, rocky passage.." and we used go command to proceed further. On next screen we got message like "You decide you explore and push.." and we used go command. On the next screen we got message like "You move towards the door..." and we used go command. On the next screen we got message like "The room has a bed, a table, and a chair" and we used go command again. On the next screen we got message like "You

come out to a corridor." and we used go command. On the next screen we got message like "The door leads to a wide room.... wand in his hand..." and we used $give$ command. On the next screen we got message like "You quickly take out your wand and offer...." and we used $read$ command to proceed further. After this we got hashed values of our password.

-Useful information which we got on the screen was as follows :
(1) Hashed password : "22 99 12 109 96 77 112 24 120 2 70 17 88 13 116 79 84 101 113 48 108 65 45 2 60 84 32 10 60 62 42 87 ".
(2) Hash values of password is made from alphabets ranging from [$f - u$].
(3) Letters are used in alphabetical order.
(4) Password is viewed as numbers $x_1, x_2, ..., x_m$ in the field F_{127}.
(5) The i^{th} number of the hashed sequence equals $x_1^{i-1} + x_2^{i-1} + ... + x_m^{i-1}$.
(6) There are 32 such numbers for i = 1 to 32.

$\longrightarrow$ The i^{th} number of the hashed sequence equals $x_1^{i-1} + x_2^{i-1} + ... + x_m^{i-1}$. (Equation-1)

$\longrightarrow x_1 = x_1^{1-1} + x_2^{1-1} + ... + x_m^{1-1}$ (put i=1)

$\longrightarrow x_1 = x_1^0 + x_2^0 + ... + x_m^0$
$\longrightarrow 22 = x_1^0 + x_2^0 + ... + x_m^0 (x_1 = 22)$
$\longrightarrow 22 = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$
$\longrightarrow$ We got $m = 22$

$\Longrightarrow$ As now we have our password length as 22, We thought to apply Brute Force approach to extract password. As it was mentioned in the instructions that the letters in the password are in alphabetical order, Therefore rather than trying all possible combinations that satisfy our hashed values, we tried the combinations in ascending and checked whether they satisfy our hashed password or not. If yes, then proceed further. Else, try another combination.

$\Longrightarrow$ In-order to speed-up the Brute-Force approach, instead of checking the validness and satisfiability of each hashed value, we checked this validness for some of the x_i's(like i=1:15) and we got a small set of passwords. We checked the passwords one by one from that set and one of them was a valid password allowing us to clear the level.

$\Longrightarrow$Final password that we got was $fghhiiijjkllllnprsssu$

No files uploaded

Q4 Password

15 Points

What was the final command used to clear this level?

fghhiiijjkllllnprsssu

Q5 Codes

0 Points

It is MANDATORY that you upload the codes used in the cryptanalysis. If you fail to do so, you will be given 0 for the entire assignment.

BonusINSYNC.zip Download

```
1  Binary file hidden. You can download it using the button
   above.
```

GROUP

Aman Mittal
Piyush Gangle
Punit Chaudhari
View or edit group

TOTAL POINTS

45 / 50 pts

QUESTION 1

Team Name **0** / 0 pts

QUESTION 2

Commands **5** / 5 pts

QUESTION 3

Analysis **25** / 30 pts

QUESTION 4

Password **15** / 15 pts

QUESTION 5

Codes **0** / 0 pts